

FORM PTO-1390 (Modified)
(REV 11-98)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US)
CONCERNING A FILING UNDER 35 U.S.C. 371

11345.023001

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR

09/622137 ✓

INTERNATIONAL APPLICATION NO.

PCT/IB99/00303

INTERNATIONAL FILING DATE

11 February 1999 (11.02.99)

PRIORITY DATE CLAIMED

13 February 1998 (13.02.98)

TITLE OF INVENTION

METHOD AND APPARATUS FOR RECORDING OF ENCRYPTED DIGITAL DATA ✓

APPLICANT(S) FOR DO/EO/US

MAILLARD, Michel and BENARDEAU, Christian ✓

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
 - a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☒ has been transmitted by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ A copy of the International Search Report (PCT/ISA/210).
8. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
 - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ have been transmitted by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☒ have not been made and will not be made.
9. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
10. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
11. ☒ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 13 to 20 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☒ Certificate of Mailing by Express Mail
20. ☒ Other items or information:

Copy of the PCT Written Opinion dated November 29, 1999 (29.11.99), 7 pages
Acknowledgement postcard

09/622137

PCT/IB99/00303

11345.023001

21. The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

- ☐ Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO \$970.00
- ☒ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO \$840.00
- ☐ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO \$690.00
- ☐ International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) \$670.00
- ☐ International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) \$96.00

ENTER APPROPRIATE BASIC FEE AMOUNT =

\$840.00

Surcharge of \$130.00 for furnishing the oath or declaration later than months from the earliest claimed priority date (37 CFR 1.492 (e)). ☐ 20 ☐ 30

\$0.00

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE
Total claims	25 - 20 =	5	x \$18.00
Independent claims	1 - 3 =	0	x \$78.00
Multiple Dependent Claims (check if applicable).			<input type="checkbox"/>
TOTAL OF ABOVE CALCULATIONS			=
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) (check if applicable).			<input type="checkbox"/>
SUBTOTAL			=
Processing fee of \$130.00 for furnishing the English translation later than months from the earliest claimed priority date (37 CFR 1.492 (f)). <input type="checkbox"/> 20 <input type="checkbox"/> 30			+
TOTAL NATIONAL FEE			=
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) (check if applicable).			<input checked="" type="checkbox"/>
TOTAL FEES ENCLOSED			=
			Amount to be: refunded
			charged

\$90.00

\$0.00

\$0.00

\$0.00

\$930.00

\$0.00

\$930.00

\$0.00

\$930.00

\$40.00

\$970.00

\$

\$

☒ A check in the amount of **\$970.00** to cover the above fees is enclosed.

☐ Please charge my Deposit Account No. _____ in the amount of _____ to cover the above fees.
A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **50-0591** A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Jonathan P. Osha
Registration No. 33,986
ROSENTHAL & OSHA L.L.P.
700 Louisiana Street, Suite 4550
Houston, Texas 77002

Telephone : (713) 228-8600
Facsimile : (713) 228-8778

EL521607510US

SIGNATURE

Jonathan P. Osha

NAME

33, 986

REGISTRATION NUMBER

August 11, 2000

DATE

09/622137

534 Rec'd PCT/PTO 11 AUG 2000

PATENT
ATTORNEY DOCKET NO. 11345.023001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Michel MAILLARD et al.

Art Unit:

Serial No.:

Examiner:

Filed:

Title: METHOD AND APPARATUS FOR RECORDING OF ENCRYPTED DIGITAL DATA

Box PCT Patent Application
Assistant Commissioner for Patents
Washington, DC 20231

PRELIMINARY AMENDMENT

Dear Sir:

Before examining the referenced application on the merits, please amend the application as outlined below:

In the Claims:

In claim 1, line 3, please delete "(50)".

In claim 3, line 1, please delete "or 2".

In claim 3, line 3, please delete "(52)".

In claim 3, line 3, please delete "(50)".

In claim 4, line 1, please delete "any preceding claim" and replace with -- claim 1 --.

In claim 4, line 2, please delete "(12)".

In claim 4, line 3, please delete "(50)".

In claim 5, line 1, please delete "(50)".

In claim 5, line 2, please delete "(30)".

In claim 7, line 1, please delete "any preceding claim" and replace with -- claim 1 --.



22511

PATENT TRADEMARK OFFICE

In claim 7, line 2, please delete “(21,24,25)”.

In claim 7, line 3, please delete “(50)”.

In claim 8, line 3, please delete “(50)”.

In claim 9, line 1, please delete “any preceding claim” and replace with -- claim 1-- .

In claim 9, line 2, please delete “(21,24,25)”.

In claim 9, line 3, please delete “(50)”.

In claim 10, line 2, please delete “(52)”.

In claim 10, line 3, please delete “(50)”.

In claim 11, line 1, please delete “or 10”.

In claim 11, line 1, please delete “(50)”.

In claim 12, line 1, please delete “any of claims 9, 10 or 11” and replace with --
claim 9--.

In claim 12, line 2, please delete “(21,23,24)”.

In claim 12, line 4, please delete “(50)”.

In claim 13, line 1, please delete “any of claims 9 to 12” and replace with --claim 9--.

In claim 13, line 1, please delete “(50)”.

In claim 13, line 4, please delete “(50)”.

In claim 14, line 1, please delete “(12)”.

In claim 14, line 2, please delete “(30)”.

In claim 14, line 2, please delete “(50)”.

In claim 14, line 2, please delete “(52)”.

In claim 14, line 4, please delete “(30)”.

In claim 14, line 4, please delete “(12)”.

In claim 14, line 4, please delete “(52)”.

In claim 15, line 2, please delete “(52)”.

In claim 15, line 3, please delete “(30)”.

In claim 17, line 1, please delete “(30)”.

In claim 19, line 1, please delete “any of claims 14 to 18” and replace with -- claim
14--.

In claim 19, line 2, please delete “(30)”.

In claim 19, line 5, please delete “(52)” in both instances.

In claim 20, line 2, please delete “(52)”.

In claim 21, line 1, please delete “any preceding claim” and replace with -- claim 1--.

In claim 21, line 1, please delete “(50)”.

In claim 21, line 2, please delete “(52)”.

In claim 21, line 4, please delete “(52)”.

In claim 22, line 1, please delete “(52)”.

In claim 23, line 1, please delete “any of claims 14 to 20” and replace with --claim
14--.

In claim 23, line 1, please delete “(20)”.

In claim 23, line 2, please delete “(30)”.

In claim 24, line 1, please delete “(20)”.

In claim 24, line 1, please delete “(30)”.

In claim 25, line 1, please delete “(30)”.

In claim 25, line 1, please delete “(20)”.

In claim 25, line 2, please delete “or 24”.

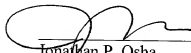
Please cancel claims 26, 27, 28 and 29.

REMARKS

The claims have been amended to remove multiple dependencies and to correct antecedent basis errors. Full examination and favorable action are requested.

Please charge any fees, or make any credits, to Deposit Account No. 500-591,
Reference No. 11345.023001

Date: 8/16


Jonathan P. Osha
Reg. No. 33,986

Rosenthal & Osha L.L.P.
700 Louisiana Street, Suite 4550
Houston, TX 77002

Telephone: 713/228-8600
Facsimile: 713/6228-8778

11345.023001.20000808.01.doc

METHOD AND APPARATUS FOR RECORDING OF ENCRYPTED
DIGITAL DATA

5 The present invention relates to a method and apparatus for recording scrambled digital data, for example television broadcasts.

10 Transmission of encrypted data is well-known in the field of pay TV systems, where scrambled audiovisual information is broadcast typically by satellite to a number of subscribers, each subscriber possessing a decoder or integrated receiver/decoder (IRD) capable of descrambling the transmitted program for subsequent viewing.

15 In a typical system, scrambled digital data is transmitted together with a control word for descrambling of the digital data, the control word itself being encrypted by an exploitation key and transmitted in encrypted form. A decoder receives the scrambled digital data and encrypted control word which uses an equivalent of the exploitation key to decrypt the encrypted control word and thereafter descramble the transmitted data. A paid-up subscriber will receive periodically the exploitation key necessary to decrypt the encrypted control word so as to permit viewing of a particular program.

20 With the advent of digital technology, the quality of the transmitted data has increased many times over. A particular problem associated with digital quality data lies in its ease of reproduction. Where a descrambled program is passed via an analogue link (e.g. the "Peritel" link) for viewing and recording by a standard VCR the quality remains no greater than that associated with a standard analogue cassette recording. 25 The risk that such a recording may be used as a master tape to make pirate copies is thus no greater than with a standard shop bought analogue cassette.

30 By way of contrast, any descrambled digital data passed by a direct digital link to one of the new generation of digital recording devices (for example, a DVHS recorder) will be of the same quality as the originally transmitted program and may thus be reproduced any number of times without any degradation of image or sound quality.

There is therefore a considerable risk that the descrambled data will be used as a master recording to make pirate copies.

French Patent Application 95 03859 shows one way of overcoming this problem, by means of a system in which descrambled digital data is never allowed to be recorded on the digital recording medium. Instead, the decoder described in this application forwards the data for recordal on the support medium in its scrambled form. The control word necessary to descramble the data is re-encrypted by means of another key and stored on the recording support with the scrambled data. This new key is known only to the receiver/decoder and replaces the exploitation key needed to obtain the control word for viewing of the program.

The advantage of such a system is that the data is never stored in a " clear " form and cannot be viewed without possession of the new key, stored in the decoder. The system also possesses the advantage that, since the exploitation key changes on a monthly basis, the use of a key chosen by the decoder to re-encrypt the control word registered on the digital tape means that the decoder will still be able to decrypt the control word recorded on the tape even after the end of a subscription month.

The disadvantage of the system proposed in this previous patent application is that the recording can only be viewed in conjunction with that particular decoder. If that decoder breaks down, or is replaced, the recording can no longer be replayed. Equally, it is not possible to play the recording directly in a digital recorder without connecting the decoder in the system.

It is an object of the present invention in its broadest and specific aspects to overcome some or all of the problems associated with this known solution.

According to the present invention, there is provided a method of recording transmitted digital data in which transmitted digital information is encrypted by a recording encryption key and stored by a recording means on a recording support medium and characterised in that an equivalent of the recording encryption key is

encrypted by a recording transport key and stored on the support medium together with the encrypted information.

5 The advantage of this method lies in the fact that the specific encryption key used to encrypt the information is itself permanently recorded with the associated encrypted information. In order to facilitate future access, and as will be described below, one or more safeguard copies of the recording transport key may be stored at another location than in the recorder.

- 10 In one embodiment, the information encrypted by the recording encryption key comprises control word information usable to descramble a scrambled data transmission also recorded on the support medium. Other embodiments are conceivable, for example, in which the encrypted information corresponds simply to transmitted data that will be ultimately read or displayed, e.g. the audiovisual
15 information itself rather than a control word used to descramble it.

- In one embodiment, the recording encryption key and/or recording transport key are stored on a portable security module associated with the recording means. This may comprise, for example, any convenient microprocessor and/or memory card device,
20 such as a PCMCIA or PC card, a smart card, a SIM card etc. In alternative realisations, the keys may be stored in a security module permanently embodied in the recording means.

- Unless explicitly limited to a portable or integrated device it is to be understood that
25 all references to a "security module" cover both possible realisations.

- In one embodiment, the transmitted information is encrypted prior to transmission and received by a decoder means before being communicated to the recording means. The decoder may be physically separate or combined with the recording means. As
30 will be explained in further detail below, the transmitted information may be in some cases processed and/or reencrypted by the decoder before being communicated to the recording means.

The decoder means may itself be associated with a portable security module used to store transmission access control keys used to decrypt the transmitted encrypted information. In some embodiments, this may be distinct from the portable security module associated with the recording means. However, in the case of an integrated
5 decoder/recorder, for example, the same security module may be used to hold all keys.

In one embodiment, the recording encryption key and/or recording transport key function in accordance with a first encryption algorithm and the transmission access
10 control keys function in accordance with a second encryption algorithm.

For example, the recording encryption and transport keys may use the symmetric DES algorithm, whilst the transmission keys function in accordance with a customised algorithm, unique to the broadcast access control system. This enables the system
15 manager to retain control over the algorithm chosen for the transmission keys whilst allowing a generic algorithm to be used for the keys relating to a recording.

In one embodiment, the recording transport key is generated at a central recording authorisation unit and a copy of this key communicated to the recording means. In
20 the event of loss or destruction of the key support associated with the recording means a backup copy or at least the means to generate the transport key will at all times be present at the central recording authorisation unit.

For security reasons, the recording transport key is preferably encrypted by a further
25 encryption key prior to being communicated to the recording means. This further encryption key may be based, for example, on an encryption key common to all recorder security modules diversified by the serial number of the security module, such that only that security module can read the message.

30 In the case where the system comprises a receiver/decoder physically separate from the recording means it may be desirable for the recording means to possess the same access rights as the receiver/decoder, for example to permit the receiver/decoder to

simply forward the data stream "as is" to the recorder for processing.

Accordingly, in one embodiment, a central access control system communicates transmission access control keys to a portable security module associated with the recording means. These may comprise, for example, a double of the keys normally held by the portable security module associated with the decoder and which are used to descramble transmissions.

In this embodiment, the recording means directly descrambles transmitted information using the transmission access keys prior to re-encryption of the information by the recording encryption key and storage on the support medium.

In a similar manner as with the communication of the transport key, the central access control system preferably encrypts the broadcast access control keys by a further encryption key prior to their communication to the recording means. This further encryption key may equally comprise an audience key common to all security modules diversified by the serial number of the recording means.

In order to enable the central access control system to correctly identify the broadcast access keys that need to be forwarded to the recording means, the recording means preferably sends a request to the central access control system including information identifying the broadcast access keys needed, the request being authenticated by the recording means using a key unique to the recording means. This may correspond, for example, to the key used to encrypt communications from the central access control system to the recording means.

In the above realisations of the invention, a number of diverse embodiments have been described, in particular in which a central recording authorisation unit generates and maintains a copy of the recording transport keys and in which a central access control system sends a duplicate set of transmission access control keys to the recording means. Alternative embodiments are possible.

For example, in one embodiment comprising a decoder means and associated security module and a recording means and associated security module, a copy of the recording transport key is stored in the security module associated with either or both decoder means or recorder means. In this way, a backup key for decrypting a recording will always be available even in the event of destruction or loss of the other security module. In particular, a copy of the recording transport key may most usefully be stored in the decoder security module.

The recording transport key may be generated, for example, by the recording means security module and communicated to the decoder means security module or vice versa. For security reasons, the recording transport key is preferably encrypted before communication to the decoder security module and decrypted by a key unique to the security module receiving the recording transport key.

This unique key and its equivalent may be embedded in the respective security modules at the moment of their creation. However, alternatively, the decoder security module and recording security module carry out a mutual authorisation process, the unique decryption key being passed to the other security module from the encrypting security module depending on the results of the mutual authorisation.

In one embodiment, the mutual authorisation step is carried out using, inter alia, an audience key known to both security modules. This may be, for example, a generic key known to all decoders and recorders and diversified by the serial number of each module.

In a further development of this double security module embodiment, the decoder means security module possesses transmission access control keys to decrypt the transmitted information in an encrypted form and a session key to re-encrypt the information prior to communication to the recording means security module, the recording means security module possessing an equivalent of the session key to decrypt the information prior to encryption by the recording transport key.

This session key may be generated by the decoder means security module or recording means security module and communicated to the other module in encrypted form using an encryption key uniquely decryptable by the other security module.

- 5 The present invention extends to a recording means for use in the above method, a decoder means and a portable security module for use in each.

The terms "scrambled" and "encrypted" and "control word" and "key" have been used at various parts in the text for the purpose of clarity of language. However, it
10 will be understood that no fundamental distinction is to be made between "scrambled data" and "encrypted data" or between a "control word" and a "key". Similarly, the term "equivalent key" is used to refer to a key adapted to decrypt data encrypted by a first mentioned key, or vice versa. Unless obligatory in view of the context or unless otherwise specified, no general distinction is made between keys associated
15 with symmetric algorithms and those associated with public/private algorithms.

The term "receiver/decoder" or "decoder" used herein may connote a receiver for receiving either encoded or non-encoded signals, for example, television and/or radio signals, which may be broadcast or transmitted by some other means. The term may
20 also connote a decoder for decoding received signals. Embodiments of such receiver/decoders may include a decoder integral with the receiver for decoding the received signals, for example, in a "set-top box", such a decoder functioning in combination with a physically separate receiver, or such a decoder including additional functions, such as a web browser or integrated with other devices such as
25 a video recorder or a television.

As used herein, the term "digital transmission system" includes any transmission system for transmitting or broadcasting for example primarily audiovisual or multimedia digital data. Whilst the present invention is particularly applicable to a
30 broadcast digital television system, the invention may also be applicable to a fixed telecommunications network for multimedia internet applications, to a closed circuit television, and so on.

As used herein, the term "digital television system" includes for example any satellite, terrestrial, cable and other system.

There will now be described, by way of example only, a number of embodiments of the invention, with reference to the following figures, in which:

Figure 1 shows the overall architecture of a digital TV system according to this embodiment;

Figure 2 shows the architecture of the conditional access system of Figure 1;

Figure 3 shows the encryption levels in the conditional access system;

Figure 4 shows the layout of a decoder and digital recording device according to this embodiment;

Figure 5 shows in schematic form the organisation of zones within the memory cards associated with the decoder and recorder of Figure 4;

Figures 6 and 7 show the steps in the preparation of messages for communication between the decoder card and a centralised server in this first embodiment;

Figure 8 shows the cryptology architecture of the decoder card in generating a recording encryption key according to this first embodiment;

Figures 9 and 10 show the preparation of ECM and EMM messages for recordal on the digital recording support according to this first embodiment;

Figure 11 shows the decryption steps associated with the replay of a recording in this first embodiment;

Figure 12 shows in schematic form the organisation of zones within the memory cards

of the decoder and recording device according to a second embodiment of the invention;

Figures 13 and 14 show the initial mutual authorisation steps and transfer of data between the decoder memory card and the recorder memory card according to this second embodiment;

Figure 15 shows the creation and communication of a session key to be used by both memory cards during recording of a programme in this second embodiment;

Figure 16 shows the operation of the recorder card to generate a recording encryption key in this second embodiment;

Figure 17 shows the treatment of transmission ECMs by the decoder card in order to communicate the control word CW in encrypted form to the recorder card in this second embodiment;

Figures 18 and 19 show the preparation of ECM and EMM messages for recordal on the digital recording support according to this second embodiment; and

Figure 20 shows communication between a decoder card and recorder card.

An overview of a digital television broadcast and reception system 1 is shown in Figure 1. The invention includes a mostly conventional digital television system 2 which uses the MPEG-2 compression system to transmit compressed digital signals. In more detail, MPEG-2 compressor 3 in a broadcast centre receives a digital signal stream (for example a stream of audio or video signals). The compressor 3 is connected to a multiplexer and scrambler 4 by linkage 5. The multiplexer 4 receives a plurality of further input signals, assembles one or more transport streams and transmits compressed digital signals to a transmitter 6 of the broadcast centre via linkage 7, which can of course take a wide variety of forms including telecom links.

The transmitter 6 transmits electromagnetic signals via uplink 8 towards a satellite

transponder 9, where they are electronically processed and broadcast via a notional downlink 10 to earth receiver 11, conventionally in the form of a dish owned or rented by the end user. The signals received by receiver 11 are transmitted to an integrated receiver/decoder 12 owned or rented by the end user and connected to the end user's television set 13. The receiver/decoder 12 decodes the compressed MPEG-2 signal into a television signal for the television set 13.

A conditional access system 20 is connected to the multiplexer 4 and the receiver/decoder 12, and is located partly in the broadcast centre and partly in the decoder. It enables the end user to access digital television broadcasts from one or more broadcast suppliers. A smartcard, capable of decrypting messages relating to commercial offers (that is, one or several television programmes sold by the broadcast supplier), can be inserted into the receiver/decoder 12. Using the decoder 12 and smartcard, the end user may purchase events in either a subscription mode or a pay-per-view mode.

An interactive system 17, also connected to the multiplexer 4 and the receiver/decoder 12 and again located partly in the broadcast centre and partly in the decoder, may be provided to enable the end user to interact with various applications via a modammed back channel 16.

The conditional access system 20 will now be described in more detail. With reference to Figure 2, in overview the conditional access system 20 includes a Subscriber Authorization System (SAS) 21. The SAS 21 is connected to one or more Subscriber Management Systems (SMS) 22, one SMS for each broadcast supplier, by a respective TCP-IP linkage 23 (although other types of linkage could alternatively be used). Alternatively, one SMS could be shared between two broadcast suppliers, or one supplier could use two SMSs, and so on.

First encrypting units in the form of ciphering units 24 utilising "mother" smartcards 25 are connected to the SAS by linkage 26. Second encrypting units again in the form of ciphering units 27 utilising mother smartcards 28 are connected to the

5 multiplexer 4 by linkage 29. The receiver/decoder 12 receives a portable security module, for example in the form of "daughter" smartcard 30. It is connected directly to the SAS 21 by Communications Servers 31 via the modammed back channel 16. The SAS sends, amongst other things, subscription rights to the daughter smartcard on request.

10 The smartcards contain the secrets of one or more commercial operators. The "mother" smartcard encrypts different kinds of messages and the "daughter" smartcards decrypt the messages, if they have the rights to do so.

15 The first and second ciphering units 24 and 27 comprise a rack, an electronic VME card with software stored on an EEPROM, up to 20 electronic cards and one smartcard 25 and 28 respectively, for each electronic card, one card 28 for encrypting the ECMs and one card 25 for encrypting the EMMs.

20 The operation of the conditional access system 20 of the digital television system will now be described in more detail with reference to the various components of the television system 2 and the conditional access system 20.

20 Multiplexer and Scrambler

25 With reference to Figures 1 and 2, in the broadcast centre, the digital audio or video signal is first compressed (or bit rate reduced), using the MPEG-2 compressor 3. This compressed signal is then transmitted to the multiplexer and scrambler 4 via the linkage 5 in order to be multiplexed with other data, such as other compressed data.

30 The scrambler generates a control word used in the scrambling process and included in the MPEG-2 stream in the multiplexer. The control word is generated internally and enables the end user's integrated receiver/decoder 12 to descramble the programme.

Access criteria, indicating how the programme is commercialised, are also added to

the MPEG-2 stream. The programme may be commercialised in either one of a number of "subscription" modes and/or one of a number of "Pay Per View" (PPV) modes or events. In the subscription mode, the end user subscribes to one or more commercial offers, or "bouquets", thus getting the rights to watch every channel
5 inside those bouquets. In the preferred embodiment, up to 960 commercial offers may be selected from a bouquet of channels.

In the Pay Per View mode, the end user is provided with the capability to purchase events as he wishes. This can be achieved by either pre-booking the event in advance
10 ("pre-book mode"), or by purchasing the event as soon as it is broadcast ("impulse mode"). In the preferred embodiment, all users are subscribers, whether or not they watch in subscription or PPV mode, but of course PPV viewers need not necessarily be subscribers.

15 Entitlement Control Messages

Both the control word and the access criteria are used to build an Entitlement Control Message (ECM). This is a message sent in relation with a scrambled program; the message contains a control word (which allows for the descrambling of the program)
20 and the access criteria of the broadcast program. The access criteria and control word are transmitted to the second encrypting unit 27 via the linkage 29. In this unit, an ECM is generated, encrypted and transmitted on to the multiplexer and scrambler 4. During a broadcast transmission, the control word typically changes every few seconds, and so ECMs are also periodically transmitted to enable the changing control
25 word to be descrambled. For redundancy purposes, each ECM typically includes two control words; the present control word and the next control word.

Each service broadcast by a broadcast supplier in a data stream comprises a number of distinct components; for example a television programme includes a video
30 component, an audio component, a sub-title component and so on. Each of these components of a service is individually scrambled and encrypted for subsequent broadcast to the transponder 9. In respect of each scrambled component of the

service, a separate ECM is required. Alternatively, a single ECM may be required for all of the scrambled components of a service. Multiple ECMs are also generated in the case where multiple conditional access systems control access to the same transmitted program.

5

Entitlement Management Messages (EMMs)

The EMM is a message dedicated to an individual end user (subscriber), or a group of end users. Each group may contain a given number of end users. This
10 organisation as a group aims at optimising the bandwidth; that is, access to one group can permit the reaching of a great number of end users.

Various specific types of EMM can be used. Individual EMMs are dedicated to individual subscribers, and are typically used in the provision of Pay Per View
15 services; these contain the group identifier and the position of the subscriber in that group.

Group subscription EMMs are dedicated to groups of, say, 256 individual users, and are typically used in the administration of some subscription services. This EMM
20 has a group identifier and a subscribers' group bitmap.

Audience EMMs are dedicated to entire audiences, and might for example be used by a particular operator to provide certain free services. An "audience" is the totality of subscribers having smartcards which bear the same conditional access system
25 identifier (CA ID). Finally, a "unique" EMM is addressed to the unique identifier of the smartcard.

EMMs may be generated by the various operators to control access to rights associated with the programs transmitted by the operators as outlined above. EMMs
30 may also be generated by the conditional access system manager to configure aspects of the conditional access system in general.

Programme Transmission

The multiplexer 4 receives electrical signals comprising encrypted EMMs from the SAS 21, encrypted ECMs from the second encrypting unit 27 and compressed programmes from the compressor 3. The multiplexer 4 scrambles the programmes and sends the scrambled programmes, the encrypted EMMs and the encrypted ECMs to a transmitter 6 of the broadcast centre via the linkage 7. The transmitter 6 transmits electromagnetic signals towards the satellite transponder 9 via uplink 8.

Programme Reception

The satellite transponder 9 receives and processes the electromagnetic signals transmitted by the transmitter 6 and transmits the signals on to the earth receiver 11, conventionally in the form of a dish owned or rented by the end user, via downlink 10. The signals received by receiver 11 are transmitted to the integrated receiver/decoder 12 owned or rented by the end user and connected to the end user's television set 13. The receiver/decoder 12 demultiplexes the signals to obtain scrambled programmes with encrypted EMMs and encrypted ECMs.

If the programme is not scrambled, that is, no ECM has been transmitted with the MPEG-2 stream, the receiver/decoder 12 decompresses the data and transforms the signal into a video signal for transmission to television set 13.

If the programme is scrambled, the receiver/decoder 12 extracts the corresponding ECM from the MPEG-2 stream and passes the ECM to the "daughter" smartcard 30 of the end user. This slots into a housing in the receiver/decoder 12. The daughter smartcard 30 controls whether the end user has the right to decrypt the ECM and to access the programme. If not, a negative status is passed to the receiver/decoder 12 to indicate that the programme cannot be descrambled. If the end user does have the rights, the ECM is decrypted and the control word extracted. The decoder 12 can then descramble the programme using this control word. The MPEG-2 stream is decompressed and translated into a video signal for onward transmission to television

set 13.

Subscriber Management System (SMS)

- 5 A Subscriber Management System (SMS) 22 includes a database 32 which manages, amongst others, all of the end user files, commercial offers, subscriptions, PPV details, and data regarding end user consumption and authorization. The SMS may be physically remote from the SAS.
- 10 Each SMS 22 transmits messages to the SAS 21 via respective linkage 23 which imply modifications to or creations of Entitlement Management Messages (EMMs) to be transmitted to end users.
- 15 The SMS 22 also transmits messages to the SAS 21 which imply no modifications or creations of EMMs but imply only a change in an end user's state (relating to the authorization granted to the end user when ordering products or to the amount that the end user will be charged).
- 20 The SAS 21 sends messages (typically requesting information such as call-back information or billing information) to the SMS 22, so that it will be apparent that communication between the two is two-way.

Subscriber Authorization System (SAS)

- 25 The messages generated by the SMS 22 are passed via linkage 23 to the Subscriber Authorization System (SAS) 21, which in turn generates messages acknowledging receipt of the messages generated by the SMS 21 and passes these acknowledgements to the SMS 22.
- 30 In overview the SAS comprises a Subscription Chain area to give rights for subscription mode and to renew the rights automatically each month, a Pay Per View Chain area to give rights for PPV events, and an EMM Injector for passing EMMs

created by the Subscription and PPV chain areas to the multiplexer and scrambler 4, and hence to feed the MPEG stream with EMMs. If other rights are to be granted, such as Pay Per File (PPF) rights in the case of downloading computer software to a user's Personal Computer, other similar areas are also provided.

One function of the SAS 21 is to manage the access rights to television programmes, available as commercial offers in subscription mode or sold as PPV events according to different modes of commercialisation (pre-book mode, impulse mode). The SAS 21, according to those rights and to information received from the SMS 22, generates EMMs for the subscriber.

The EMMs are passed to the Ciphering Unit (CU) 24 for ciphering with respect to the management and exploitation keys. The CU completes the signature on the EMM and passes the EMM back to a Message Generator (MG) in the SAS 21, where a header is added. The EMMs are passed to a Message Emitter (ME) as complete EMMs. The Message Generator determines the broadcast start and stop time and the rate of emission of the EMMs, and passes these as appropriate directions along with the EMMs to the Message Emitter. The MG only generates a given EMM once; it is the ME which performs cyclic transmission of the EMMs.

On generation of an EMM, the MG assigns a unique identifier to the EMM. When the MG passes the EMM to the ME, it also passes the EMM ID. This enables identification of a particular EMM at both the MG and the ME.

In systems such as simulcrypt which are adapted to handle multiple conditional access systems e.g. associated with multiple operators, EMM streams associated with each conditional access system are generated separately and multiplexed together by the multiplexer 4 prior to transmission.

Encryption Levels of the System

Referring now to Figure 3, a simplified outline of the encryption levels in the

broadcast system will now be described. The stages of encryption associated with the broadcast of the digital data are shown at 41, the transmission channel (eg a satellite link as described above) at 42 and the stages of decryption at the receiver at 43.

- 5 The digital data N is scrambled by a control word CW before being transmitted to a multiplexer Mp for subsequent transmission. As will be seen from the lower part of Figure 3, the transmitted data includes an ECM comprising, inter alia, the control word CW as encrypted by an encrypter Ch1 controlled by a first encryption key Kex. At the receiver/decoder, the signal passes by a demultiplexer DMP and descrambler
- 10 D before being passed to a television 2022 for viewing. A decryption unit DCh1 also possessing the key Kex decrypts the ECM in the demultiplexed signal to obtain the control word CW subsequently used to descramble the signal.

- For security reasons, the control word CW embedded in the encrypted ECM changes
- 15 on average every 10 seconds or so. In contrast, the first encryption key Kex used by the receiver to decode the ECM is changed every month or so by means of an operator EMM. The encryption key Kex is encrypted by a second unit ChP using a personalised group key K1(GN). If the subscriber is one of those chosen to receive an updated key Kex, a decryption unit DChP in the decoder will decrypt the message
- 20 using its group key K1(GN) to obtain that month's key Kex.

- The decryption units DChp and DCh1 and the associated keys are held on a smart card provided to the subscriber and inserted in a smart card reader in the decoder. The keys may be generated, for example, according to any generally used symmetric
- 25 key algorithm or in accordance with a customised symmetric key algorithm.

- As will be described, different keys may be associated with different operators or broadcasters as well as with the conditional access system supplier. In the above description, a group key K1(GN) is held by the smart card associated with the
- 30 decoder and used to decrypt EMM messages. In practice, different operators will have different subscriber unique keys K1 (Op1, GN), K1 (Op2, GN) etc. Each group key is generated by an operator and diversified by a value associated with the group

to which the subscriber belongs. Different memory zones in the smart card hold the keys for different operators. Each operator may also have a unique key associated solely with the smart card in question and an audience key for all subscribers to the services provided by that operator (see above).

5

In addition, a set of keys may also be held by the manager of the conditional access system. In particular, a given smart card may include a user specific key K0 (NS) and an audience key K1 (C), common to all smart cards. Whilst the operator keys are generally used to decode EMM messages associated with broadcast rights, the conditional access manager keys may be used to decrypt EMM messages associated with changes to conditional access system in general, as will be described below.

10

The above description of the system shown in Figure 3 relates to the implementation of access control in a broadcast system in which transmissions are descrambled by a decoder and displayed immediately. Referring to Figure 4, the elements of an access control system for recording and replaying of scrambled transmission will now be described.

15

As before, a decoder 12 receives scrambled broadcast transmissions via a receiver 11. The decoder includes a portable security module 30, which may conveniently take the form of a smart card, but which may comprise any other suitable memory or microprocessor device. The decoder 12 includes a modem channel 16, for example, for communicating with servers handling conditional access information and is also adapted to pass descrambled audiovisual display information, e.g. via a Peritel link 53, to a television 13. The system additionally includes a digital recorder 50, such as a DVHS or DVD recorder, adapted to communicate with the decoder, for example, via an IEEE 1394 bus 51. The recorder 50 receives a digital support (not shown) on which information is recorded.

20

25

The recorder 50 is further adapted to function with a portable security module 52 containing, inter alia, the keys used to control access to the replaying of a recording. The portable security module may comprise any portable memory and/or

30

microprocessor device as is conventionally known, such as a smart card, a PCMCIA card, a microprocessor key etc. In the present case, the portable security module 52 has been designated as a SIM card, known from the field of portable telephones.

5 The digital recorder 50 includes a direct link 54 to the display 13. In alternative realisations, digital audiovisual information may be passed from the recorder 50 to the decoder 12 prior to display. Equally, whilst the elements of decoder 12, recorder 50 and display 13 have been indicated separately, it is conceivable that some or all of these elements may be merged, for example, to provide a combined
10 decoder/television set or combined decoder/recorder etc.

Similarly, whilst the invention will be discussed in relation to the recording of audiovisual broadcast information, it may also conveniently be applied, for example, to broadcast audio information subsequently recorded on a DAT or minidisc recorder
15 or even a broadcast software application recorded on the hard disc of a computer.

A first and second embodiment of the invention will now be described with reference to Figures 5 to 11 and 12 to 19, respectively. In the first embodiment a central server is used to handle the generation and safeguard of the keys permitting access
20 to a recording. Furthermore, in this embodiment, the real time decryption and descrambling of a broadcast is carried out by the SIM card of the recorder prior to recordal. In the second embodiment, the decoder smart card manages the safeguard of recording access keys and also plays a part in the real time decryption and decoding of broadcast transmissions.

25

First Embodiment

Referring to Figure 5, the structure of the memory zones in the smart card 30 and SIM card 52 associated with the decoder and recorder, respectively, will now be
30 described.

As shown, the decoder smart card 30 includes a number of keys adapted to function

with a symmetric encryption/decryption algorithm associated with the conditional access system. In the present example, a custom algorithm "CA" is used for operations generally associated with access to the broadcast transmission. This is to distinguish from the operations carried out by the SIM card 52 using the DES algorithm and which are generally associated with the recordal and playback of information on the digital support (see below).

The first set of keys, associated with the conditional access system manager indicated in the zone 55, are implanted in the smart card at the moment of personalisation.

These keys include a key K0 diversified by a number NS unique to that card. The system manager zone 55 may also include other keys, such as an audience key K1 (not shown) diversified by a constant C and common to all smart cards handled by the conditional access system manager.

A second zone 56 contains the keys associated with one or more broadcast operators. These keys may be implanted at the moment of personalisation of the card 30 by the conditional access system manager but are more usually created by means of a special transmitted EMM message at the start up of a decoder.

As mentioned above, the operator keys may typically include a K0' diversified by a number NS unique to that card, a group key K1' diversified by a group number GN and an audience key K2' diversified by a constant Z and common to all subscriber card addressed by that operator.

Finally, the smart card includes the value of the unique number NS of that card, implanted at the moment of personalisation and held in the zone 57 of the smart card memory.

As is shown, the SIM card 52 associated with the digital recorder includes two sections 58, 59 associated with keys and operations carried out using the CA and DES algorithms, respectively. The section 59 associated with operations using the CA algorithm includes a first system manager zone 60 and an operator zone 61. The

keys in the system manager zone are implanted in the card at the moment of personalisation by the conditional access system manager and include a key K0 diversified by the serial number NSIM of the SIM card as well as a communications transport key T also diversified by the serial number NSIM of the card. Both keys
5 are unique to the SIM card in question.

The SIM card further includes an operator zone 61 adapted to store keys associated with one or more operators. In the present Figure 5, the SIM card is shown as it is at the moment of its creation and personalisation by the conditional access system
10 manager and before insertion in a recorder. For this reason, both the operator zone 61 and the DES zone 58 are shown as blank, i.e. without any stored keys.

Finally, the SIM card includes a zone 63 adapted to hold the unique SIM card serial number NSIM.
15

As mentioned above, in this embodiment, the recorder SIM card 52 is adapted to handle the real time decryption and descrambling of broadcast data autonomously and independent of the smart card 30 associated with the decoder. In order to carry out these operations, it is necessary for the recorder SIM card 52 to possess a double of
20 the keys usually held in the system manager and operator zones 55, 56 of the decoder smart card (see Figure 5). As will be described, once the necessary keys are installed in the recorder SIM card 52, the decoder 12 will thereafter pass the broadcast transmission stream "as is" to the digital recorder 50 and card 52.

In this embodiment, the generation of duplicate broadcast related keys is managed by the central conditional access system 21, the digital recorder 50 acting to transmit a request to the appropriate server, e.g. via the modem link provided by the decoder 12. Alternatively, it may be envisaged that the recorder itself will be equipped with a modem to carry out this request. In this embodiment, the central conditional access
30 system serves to regulate both transmission access control keys and, as will be described recording access control keys

In order to enable the central conditional access system server to generate a double of the keys associated with the decoder smart card it is necessary that the request message from the recorder SIM card includes an identification of the identity of the decoder smart card (e.g. the smart card serial number NS) as well as providing
5 secured confirmation of its own identity.

As a first step therefore, the decoder smart card 30 communicates its serial number NS and a list of operators Op1, Op2 etc. to the SIM card 52. For reasons of security, this communication may itself be encrypted by a simple transport encryption
10 algorithm applied to all communications between the decoder 12 and recorder 50. To avoid unnecessary complexity in the Figures, the keys associated with this encryption are not shown. The decoder card serial number NS is then stored in the system manager zone of the SIM card.

15 The recorder SIM card 52 then sets up a communication with the conditional access system 21 and requests the unique number NMERE of the conditional access system 21 at the conditional access server (see Figure 2). Using the information thus obtained, the recorder SIM card 52 generates a message using the CA algorithm, as shown in Fig. 6.

20 In the convention adopted in the accompanying drawings, the symmetric algorithm to be used in a given cryptographic step (CA or DES) is identified within an oval. The data to be encrypted and/or the data serving as a diversifier is identified as arriving via a blacked out input to the oval. See the encryption of the smart card
25 number and operator list at 70 in Figure 6. Decryption steps are distinguished using an inverse power sign, for example CA^{-1} or DES^{-1} .

As a first step in Figure 6, the smart card number NS and operator list are encrypted by the key K0 (NSIM) as shown at 70 to generate a message 71 comprising the SIM
30 card serial number NSIM and the encrypted data. At a second step 72, the encrypted data is again re-encrypted by the key T (NSIM, NMERE), created by diversifying the key T (NSIM) by a unique value NMERE associated with the conditional access

system. As will be understood, the steps 70, 71 may be carried out in the inverse order. The message 73 and signature thus formed are then sent to the conditional access server 21, ciphering unit 24 and mother card 25.

- 5 The conditional access system 21 decrypts the message as shown in Figure 7. The system possesses the original key K0 shown at 76. Diversifying the key K0 with the NSIM value contained in the message, as shown at 77, generates the key K0 (NSIM). The key K0 (NSIM) is first used to validate the signature at 78. In the event that the signature is not valid, the analysis of the message ends, as shown at 81.

10

In addition to the key K0, the system also possesses the transport key T or at least the key T (NMERE) representing the value of this key T diversified by unique conditional access system number NMERE. Diversifying T (NMERE) by the value NSIM contained in the message enables the system to generate the key T (NSIM, NMERE). For the sake of simplicity, the steps in the preparation of this key have not been shown in Figure 7.

15

- Equipped with keys K0 (NSIM) and T (NSIM, NMERE), the system manager can then decrypt the message at 79 to obtain the decoder smart card serial number NS and the list of operators associated with the subscriber in question. The system manager then further verifies that the list of operators does indeed match the smart card serial number and thereafter assembles in an EMM message the duplicate key values that will be needed by the recorder SIM card to decrypt a transmission, including a duplicate of the smart card system manager key K0 (NS) as well as the various operator keys K0' (Op1, NS), K1' (Op1, GN) etc.

20

25

- The access system also prepares a recording transport key RT (A) which will be subsequently used by the SIM card in controlling access during the recording and playback of a digital recording, as will be discussed in more detail below. In accordance with the choice of algorithm preferred for dealing with the recording, this key will be prepared from a DES key RT diversified by a random number A. The key RT is always present in the mother card and a copy of the value A is maintained

30

for safeguard purposes in a database associated with the system operator. In this way, the value RT (A) may be regenerated at any moment.

The smart card duplicate keys K0 (NS), K0' (Op1, NS), Kex etc. and the recording transport key RT (A) are then formatted into an EMM message sent to the recorder SIM card. For security reasons, this message is encrypted by the key K0 (NSIM) to ensure that only the correct SIM card can obtain this information.

For any subsequent change or update, for example, in relation to the operator keys or other access rights, the SIM card (as a copy of the smart card) will receive all EMM/ECM messages needed to decrypt broadcast transmissions.

Referring to Figure 8, the state of the recorder SIM card 52 immediately prior to the recording of a broadcast transmission will now be described. As shown, the digital recorder card 59 now includes complete system manager and operator zones 60, 61 as well as a stored value the DES recording transport key RT (A) shown at 85. In addition, the card generates a recording encryption key E (NE) shown at 86 and obtained by diversifying at 87 a DES key E shown at 88 by a random value NE shown at 89. In this case, the key E(NE) is used as a type of session key and may be changed between recordings. The pair of keys E (NE) and RT (A) will subsequently be used in all encryption and decryption of the digital recording.

Referring to Figure 9, the steps in the treatment by the recorder of an ECM message associated with a broadcast transmission will now be described. After the arrival of an ECM message at 90, the card verifies at 91 that it has the rights to read this particular transmission, for example, that it is a transmission from one of the operators in its list of operators. If so, the encrypted control word CW is extracted from the ECM at the step 92. If not, the processing stops at step 93. Using that month's exploitation key Kex for the operator in question shown at 94, the card decodes at 95 the encrypted value to obtain the control word CW in clear, as shown at 96.

The recorder card then re-encrypts at 97 the control word CW using the DES key E (NE) shown at 98 and prepares an ECM including the newly encrypted control word for insertion in the data stream to replace the previous ECM. The scrambled transmission together with the sequence of new ECM messages are then recorded on the support in the digital recorder.

Simultaneously and as shown at step 101 in Figure 10, the SIM recorder card encrypts the value E (NE) shown at 100 using the recording transport key RT (A) shown at 102, so as to generate a special EMM type message 103. This EMM message is then recorded on the digital recording support at the start or header of the recording. As will be understood from the foregoing description, other than the safeguard copy held at the conditional access system database, the key RT (A) is unique to the recorder card and this EMM message may not be decrypted by cards other than the recorder card that generated the message.

Referring to Figure 11, the steps in the decryption and descrambling of a recording will now be described. Firstly, the EMM message 111 at the head of the recording is decrypted at 110 using the recording transport key 112 stored in the SIM card. Assuming the EMM message was originally created using the same recording transport key the result of the decryption step 110 will be the recording encryption key E (NE) at 116.

As the recording is played, ECMs 113 are picked out from the data stream and decrypted at step 114 using the recording encryption key E (NE) to obtain at step 115 the control word CW used to scramble that part of the data stream associated with the ECM. This control word CW is then fed together with the scrambled audiovisual data to a descrambling unit, either in the recorder SIM card or in the recorder itself, and a descrambled audiovisual output obtained for subsequent display via the television display or the like.

As will be understood, the presence of a safeguard means for preparing a copy of the transport key RT (A) at the mother card 25 of the central access control system

means that, in the event of loss or destruction of the recorder SIM card 25, it will be possible to reconstruct a new recorder card to allow playback of previously made recordings.

- 5 The above embodiment is particularised by the fact that the recording transport key RT (A) is generated and safeguarded at a central server and also by the fact that the recorder SIM card contains a duplicate of the necessary operator keys to independently decrypt and descramble a real time transmission. The second embodiment, described below in Figures 12 to 19 does not suffer from these
- 10 constraints, but describes a realisation in which the decoder smart card plays a more important role.

Second Embodiment

- 15 Referring to Figure 12, the structure of the conditional access zones in the decoder smart card 30 and recorder SIM card 52 in such a system are shown. As before, both cards include zones reserved for operations using the CA algorithm and storage of key data, in particular system manager zones 55, 60 and operator zones 56, 61.
- 20 In the present embodiment, the system manager zone 55 of the decoder card 30 includes, in addition to the key K0 (NS), an audience key K1 (C) common to all cards personalised and managed by the system manager and formed by the diversification of a CA key by a constant value C. This key K1 (C) is also present in the system management zone 60 of the recorder card 52.

25

The other significant change in comparison with the zone structure of the previous embodiment is that the smart card 30 is additionally provided with the DES algorithm and includes a DES operating zone 120.

- 30 In order to enable the decoder smart card and recorder SIM card to work together and, in particular, to enable the eventual generation of a recording transport key TR, it is necessary for a mutual authentication of both cards to be carried out.

As shown in Figure 13, as a first step 121 the recorder SIM card 52 requests a random number from the decoder smart card 30 which returns the number A1 at 122. This number is then used to diversify the audience key K1 (C) at step 123 to generate the key K1 (C, A1) shown at step 124. The SIM card then generates a second
5 random number A2 shown at 125, which is in turn encrypted by the key K1 (C, A1) at 126. Before communication to the smart card, this message is again encrypted and signed at 128 by a second key K1 (C, NSIM) shown at 127 and formed by diversifying the audience key K1 (C) by the value NSIM. The message 129 thus formed is sent as a request for serial number NS and associated individual key
10 K0(NS) to the decoder smart card 30.

Referring to Figure 14, on arrival at the decoder smart card 30, the communicated value NSIM is used by the smart card to generate the key K1 (C, NSIM). The value of A2 is then decrypted at 130 using this key and the key K1 (C, A1) obtained by the
15 smart card using the random number A1 that it had previously generated and stored in its memory.

This random number value A2 obtained at 131 is then used to diversify the audience key K1 (C) to obtain the key K1 (C, A2) shown at 132. The key K1 (C, A2) then
20 encrypts the smart card unique serial number NS and system key K0 (NS) at 133 to create the message 134.

As before, this message is then re-encrypted at 135 using the key K1 (C, NSIM) shown at 136 and the message returned to the recorder SIM card 52 as shown at 137.

25 The recorder SIM card generates the keys K1 (C, A2) and K1 (C, NSIM) shown at 138 by diversifying the key K1 (C) by the NSIM serial number and the previously generated and memorised random number A2. These keys are used to decrypt at 139 the messages so as to obtain the unique serial number NS and unique system manager
30 key K0 (NS) of the smart card, this information thereafter being recorded in the memory of the recorder SIM card at 140.

Unlike the previous embodiment, in which doubles of all system manager and operator keys were taken to ensure independent operation of the recorder SIM card, the double key K0 (NS) and the smart card serial number NS are used to set up a session key for recording and to enable secure communication between the cards during a recording session, notably to enable secure communication of a recording transport key.

In this embodiment, the initial decryption of the CW is handled by the smart card using the operator keys and monthly exploitation keys that it possesses. Whilst it is conceivable that the control word CW could be passed directly to the SIM card during the creation of a recording it is desirable for security reasons to use a session key to transport the control word CW for this purpose.

Figure 15 shows one way of creating such a key. As shown, the recorder SIM card picks a random key K3 shown at 141 and diversifies this key at 142 with the SIM card serial number NSIM shown at 143. The key K3 may be taken from any one of a number of such keys stored for this purpose in the system manager zone. The CA session key K3 (NSIM) thus created at 144 is then encrypted at 145 using the previously obtained smart card system manager key K0 (NS) shown at 146. The message 147 thus generated is thereafter transmitted to the decoder smart card 55 which uses its key K0 (NS) to decrypt the message at 148 and store the session key K3 (NSIM) in the memory of the card at step 149.

Referring to Figure 16, the state of the recorder SIM card prior to a recording operation will now be described. The system manager zone 60 includes the smart card key K0 (NS) and the session key K3 (NSIM) as well as the normally present system keys K0 (NSIM) etc. (not shown). In addition, the card creates a DES recording encryption key from a DES key E shown at 150 by diversifying this key at 151 by a random value NE shown at 152. As before, the resulting recording encryption key E (NE) will be used in the re-encryption of the control words associated with a program. Similarly, a recording transport key RT (A) shown at 153 is generated to be used to encrypt the recording encryption key E (NE) also recorded

on the digital support medium.

Unlike the previous embodiment, in which the recording transport key was generated at the access control server, the key RT (A) is generated by the recorder SIM card itself using a DES key diversified by a random number A. In order to safeguard a copy of this key a copy is communicated to the decoder smart card. For obvious security reasons, this copy is communicated in encrypted form, for example, as encrypted by the smart card key K0 (NS) currently stored in the SIM card memory.

Referring to Figure 20, upon first insertion in the decoder the recorder SIM card 52 first sends a request 190 to the smart card to see if a value of RT(A) has already been generated. An evaluation is carried out by the decoder smart card at 191.

If the answer is negative, the recorder SIM card 52 generates a random DES key RT at 192, which value is diversified at 193 by a random value A shown at 194 to generate the key RT(A) shown at 195. This key value RT(A) is then encrypted at 196 using the custom algorithm and the key K0(NS) shown at 197 and the resulting message 198 then sent to the decoder smart card 30 for decryption and safeguard of the key RT(A).

If the determination at 191 is positive, then the previously stored value of RT(A) is sent back at 199 to the recorder SIM card 52.

Referring to Figure 17, the operations of the decoder smart card 30 during recording of a scrambled transmission will now be described. As mentioned above, in this embodiment, the decoder smart card handles the initial decryption steps using the operator keys before communicating the value of the control word CW to the recorder SIM card 52.

As shown, the decoder smart card 30 receives an ECM 160 for processing in the operator zone 56. Firstly, the smart card 30 checks that it has the rights to access this program. Assuming that this is the case, the encrypted code word CW is

extracted from the ECM at 162 and decrypted at 163 using the appropriate exploitation key Kex shown at 164. Otherwise, the process ends as shown at 165.

5 As mentioned above, the clear value of the control word CW shown at 166 cannot be directly communicated to the recorder SIM card. Accordingly, the control word CW is encrypted at 167 using the session key K3 (NSIM) shown at 168 and the resulting value 169 communicated to the recorder card SIM for the next steps in the process.

10

Referring to Figure 18, the control word encrypted by the session key is received by the recorder SIM card 52 which carries out a decryption process at 170 using the equivalent of the session key K3 (NSIM) previously stored in memory shown at 171. The clear value of the control word CW at 172 is then passed to the DES zone of the card for encryption at 173 using the recording encryption key E (NE) shown at 174. The resulting encrypted value is then encapsulated in an ECM and inserted in the data stream for recordal with the still scrambled data on the recording support.

15

At the same time and in a similar manner to the first embodiment, the recording encryption key value shown at 180 in Figure 19 is encrypted at 181 using the recording transport key RT(A) shown at 182. The resulting encrypted value 183 is encapsulated in an EMM for recordal in the header of the digital recording.

20

During replay of the recording, and as described before in relation to Figure 11, the EMM at the start of a recording containing the recording encryption key E (NE) is decrypted by the recorder SIM card using the recording transport key RT (A). The recording encryption key E (NE) is then used to decrypt each ECM so as to obtain the control word CW associated with that particular section of the scrambled recording. The recording is then descrambled and played.

25

30

As will be understood, the presence of a safeguard copy of the recording transport key RT (A) stored in the decoder smart card means that, in the event of loss or

breakdown of the recorder SIM card, a replacement recorder card may be generated. Unlike the previous embodiment, however, it is not necessary to use a centralised server to maintain this duplicate copy.

- 5 As will be understood, alternative embodiments may be envisaged. For example, in the above embodiments the encryption recording key E (NE) is generated using a key and a random number. However, in alternative embodiments the key E (NE) may be generated from a key diversified by the serial number of the recording device itself (i.e. not the recorder SIM card) to link a given recording to both the recorder SIM
- 10 card and the recording device.

Similarly, certain elements of the first embodiment such as a centralised transport key store and an autonomously operating recorder are independent from each other and may be used in the second embodiment, and vice versa.

15

CLAIMS

1. A method of recording transmitted digital data in which transmitted digital information is encrypted by a recording encryption key (E(NE)) and stored by a recording means (50) on a recording support medium and characterised in that an equivalent of the recording encryption key (E(NE)) is encrypted by a recording transport key (RT(A)) and stored on the support medium together with the encrypted information.

2. A method as claimed in claim 1 in which the information encrypted by the recording encryption key (E(NE)) comprises control word information (CW) usable to descramble a scrambled data transmission also recorded on the support medium.

3. A method as claimed in claim 1 or 2 in which the recording encryption key (E(NE)) and/or recording transport key (RT(A)) are stored on a portable security module (52) associated with the recording means (50).

4. A method as claimed in any preceding claim in which the transmitted information is encrypted prior to transmission and received by a decoder means (12) before being communicated to the recording means (50).

5. A method as claimed in claim 4 in which the decoder (50) is associated with a portable security module (30) used to store transmission access control keys (K0(NS), K0'(Op1,NS) etc.) used to decrypt the transmitted encrypted information.

6. A method as claimed in claim 5 in which the recording encryption key (E(NE)) and/or recording transport key (RT(A)) function in accordance with a first encryption algorithm (DES) and the transmission access control keys (K0(NS), K0'(Op1,NS) etc.) function in accordance with a second encryption algorithm (CA).

7. A method as claimed in any preceding claim in which the recording transport key (RT(A)) is generated at a central recording authorisation unit (21,24,25) and a copy

of this key communicated to the recording means (50).

8. A method as claimed in claim 7 in which the recording transport key (RT(A)) is preferably encrypted by a further encryption key (K0(NSIM)) prior to being
5 communicated to the recording means (50).
9. A method as claimed in any preceding claim in which a central access control system (21,24,25) communicates transmission access control keys (K0(NS), K0'(Op1,NS) etc.) to the recording means (50).
10
10. A method as claimed in claim 9 in which the transmission access control keys (K0(NS), K0'(Op1,NS) etc.) are communicated to a portable security module (52) associated with the recording means (50).
11. A method as claimed in claim 9 or 10 in which the recording means (50) directly descrambles transmitted information using the transmission access keys (K0(NS), K0'(Op1,NS) etc.) prior to re-encryption of the information by the recording encryption key (E(NE)) and storage on the support medium.
15
12. A method as claimed in any of claims 9, 10 or 11 in which the central access control system (21, 24, 25) preferably encrypts the broadcast access control keys (K0(NS), K0'(Op1,NS) etc.) by a further encryption key (K0(NSIM)) prior to their communication to the recording means (50).
20
13. A method as claimed in any of claims 9 to 12 in which the recording means (50) sends a request to the central access control system including information identifying the broadcast access keys needed (K0(NS), K0'(Op1,NS) etc.), the request being authenticated by the recording means (50) using a key (K0(NSIM)) unique to that recording means.
25
14. A method as claimed in claim 1 using a decoder means (12) and associated security module (30) and a recording means (50) and associated security module (52)
30

and in which a copy of the recording transport key (RT(A)) is stored in the security module (30) associated with the decoder means (12) and/or the security module (52) associated with the recording means.

- 5 15. A method as claimed in claim 14 in which the recording transport key (RT(A)) is generated by either the recording security module (52) or decoder security module (30) and communicated to the other security module.
- 10 16. A method as claimed in claim 15 in which the recording transport key (RT(A)) is preferably encrypted before communication to the other security module and decrypted by a key unique (K0(NS)) to that other security module.
- 15 17. A method as claimed in claim 16 in which the decoder security module (30) and recording security module (52) carry out a mutual authorisation process, the unique decryption key (K0(NS)) being passed to the other security module from the encrypting security module depending on the results of the mutual authorisation.
- 20 18. A method as claimed in claim 17 in which the mutual authorisation step is carried out using, inter alia, an audience key K1(C) known to both security modules (30,52).
- 25 19. A method as claimed in any of claims 14 to 18 in which the decoder security module (30) possesses transmission access control keys (K0(NS), K0'(Op1,NS) etc.) to decrypt the transmitted information in an encrypted form and a session key (K3(NSIM)) re-encrypt the information prior to communication to the recording security module (52), the recording security module (52) possessing an equivalent of the session key (K3(NSIM)) to decrypt the information prior to encryption by the recording transport key (RT(A)).
- 30 20. A method as claimed in claim 19 in which the session key (K3(NSIM)) is generated by the decoder security module or recording means security module (52) and communicated to the other module in encrypted form using an encryption key

(K0(NS)) uniquely decryptable by the other security module.

21. A recording means (50) adapted for use in a method as claimed in any preceding claim comprising a security module (52) for encrypting transmitted digital information by a recording encryption key (E(NE)) for storage on a recording support medium and characterised in that the security module (52) is further adapted to encrypt the recording encryption key (E(NE)) by a recording transport key (RT(A)) for storage on the support medium.
- 10 22. A portable security module (52) adapted for use in the recording means of claim 21 and characterised in comprising a recording encryption key (E(NE)) for encryption of transmitted digital information for subsequent recordal and a recording transport key (RT(A)) for encryption of the recording encryption key for subsequent recordal.
- 15 23. A decoder means (20) adapted for use in a method as claimed in any of claims 14 to 20 including a security module (30) adapted to store a copy of the recording transport key (RT(A)).
- 20 24. A decoder means (20) as claimed in claim 23 including a security module (30) adapted to descramble transmitted information using one or more transmission access keys (K0(NS), K0'(Op,NS) etc.) prior to reencryption by a session key (K3(NSIM)) for subsequent communication to a recording means.
- 25 25. A portable security module (30) adapted for use in the decoder means (20) of claim 23 or 24 and comprising at least a copy of the recording transport key (RT(A)).
26. A method of recording transmitted digital data substantially as herein described.
- 30 27. A recording means substantially as herein described.
28. A portable security module substantially as herein described.

29. A decoder means substantially as herein described.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
22

Fig.1.

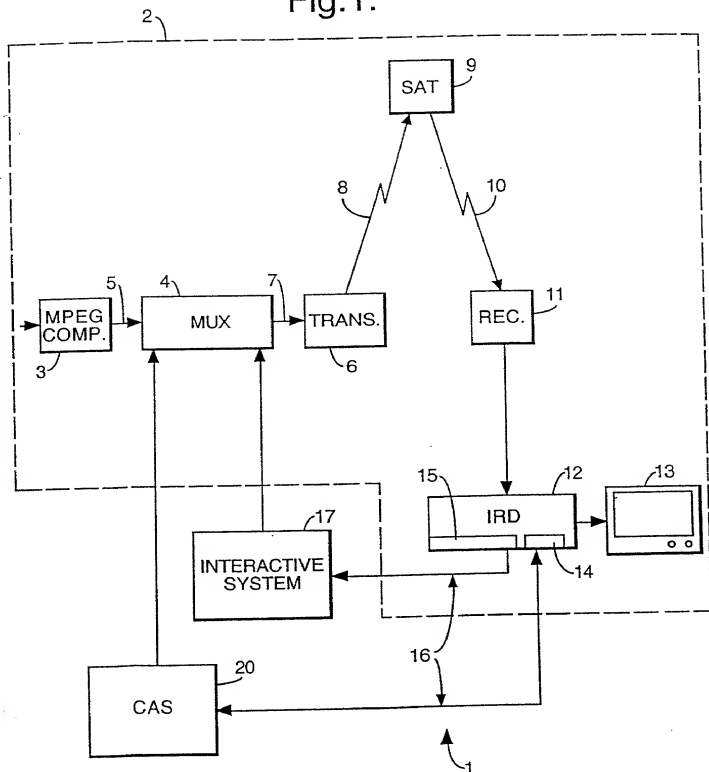


Fig.2.

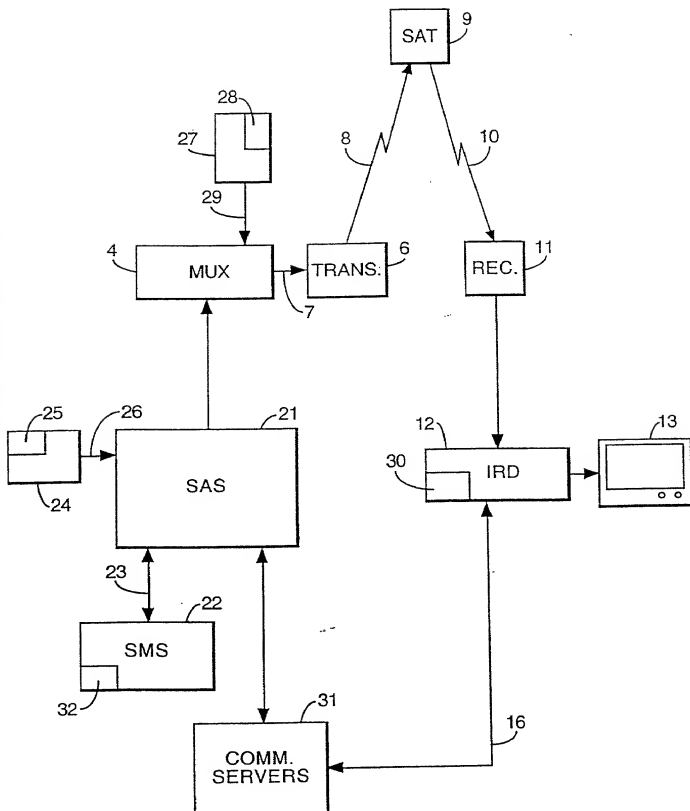


Fig.3.

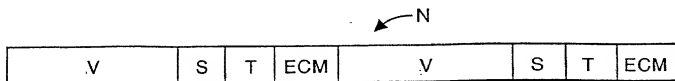
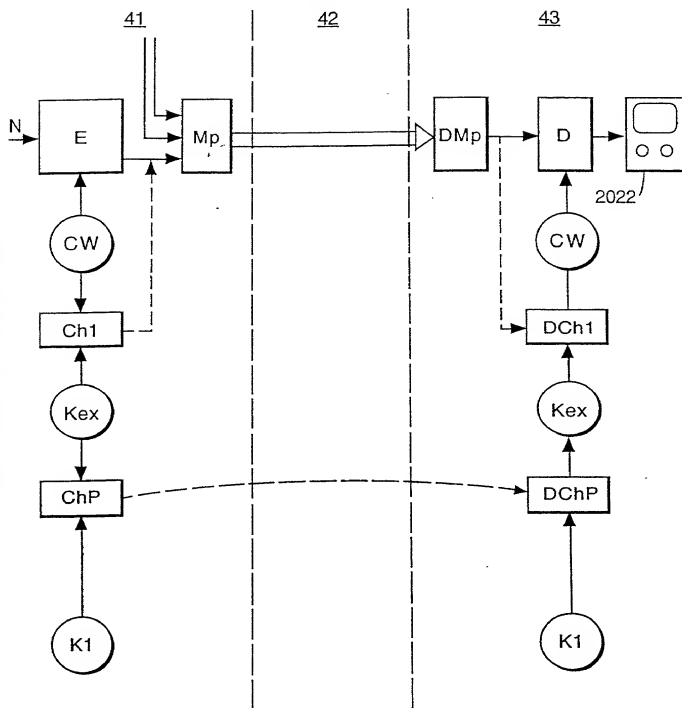


Fig.4.

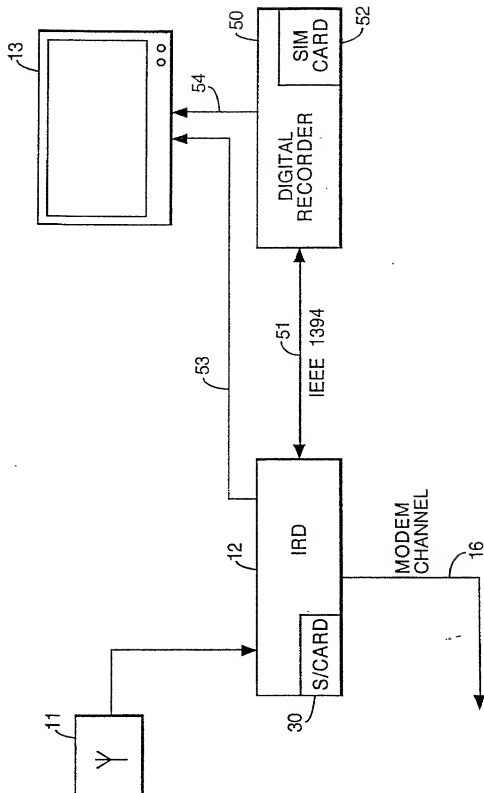


Fig.5.

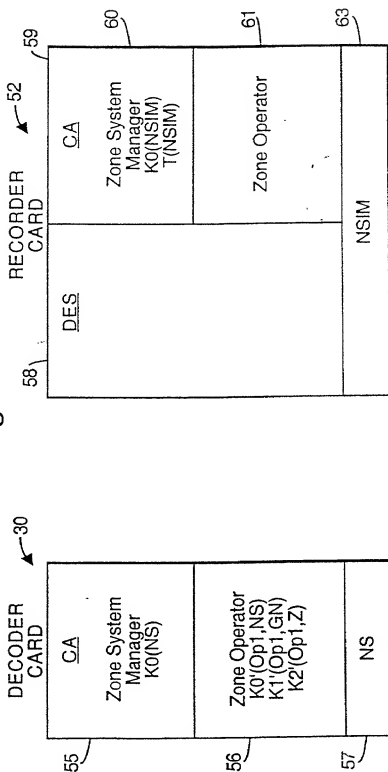


Fig.6.

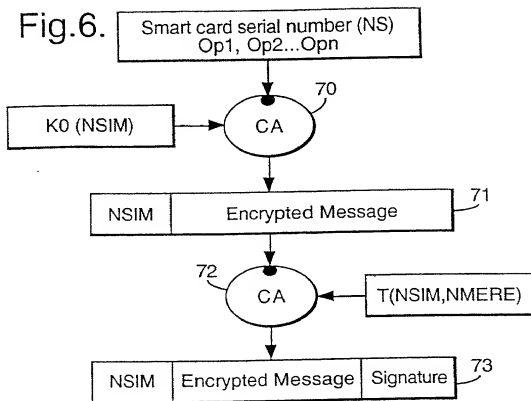


Fig.7.

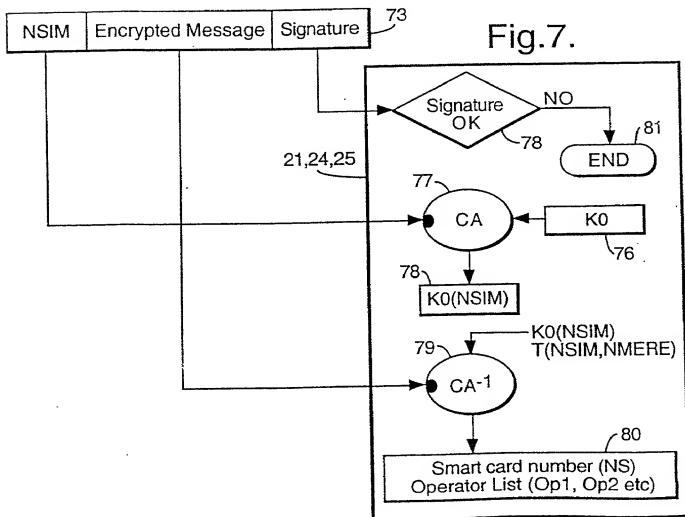


Fig.8.

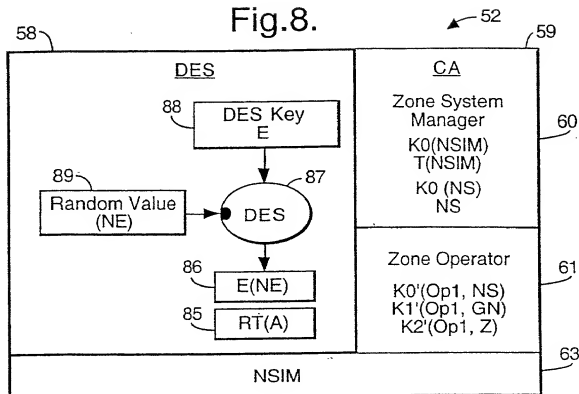
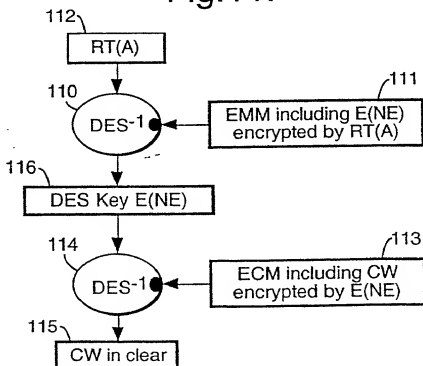


Fig.11.



8/15

Fig.9.

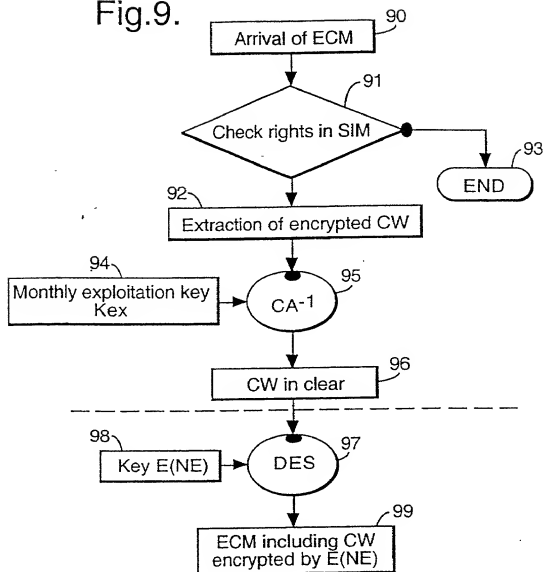


Fig.10.

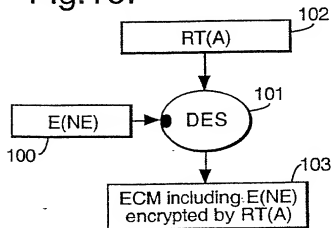
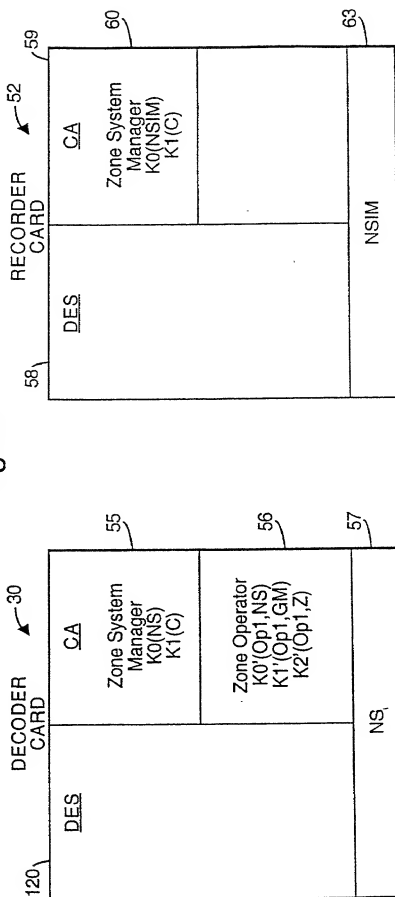
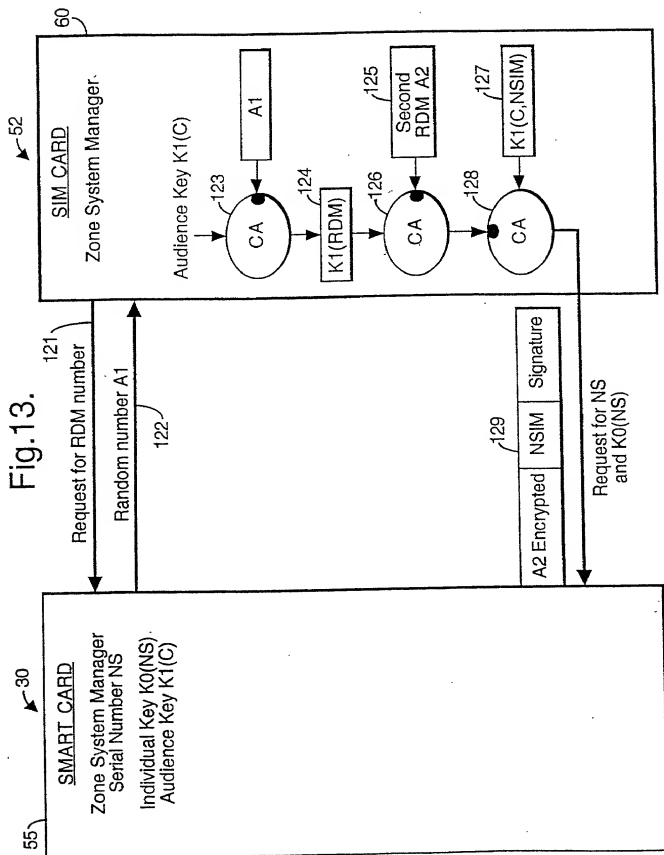
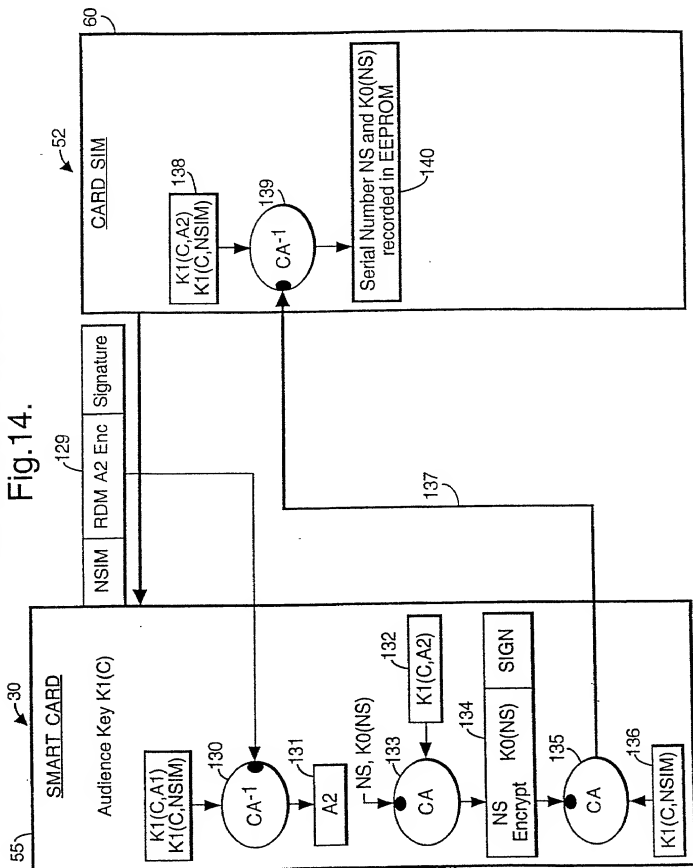


Fig.12.







12/15

Fig.15.

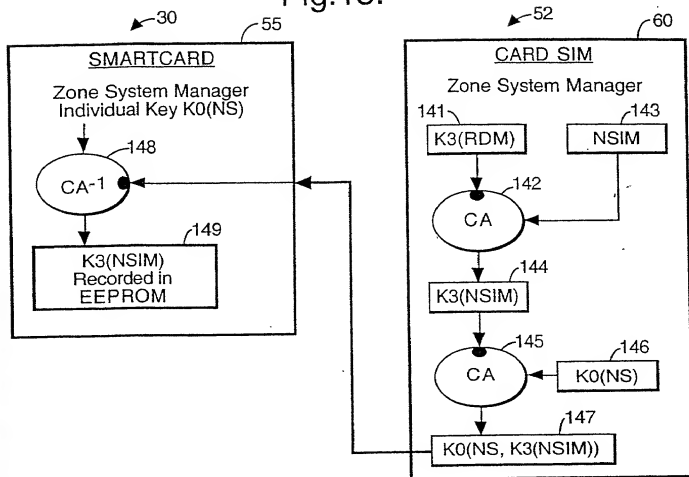


Fig.16.

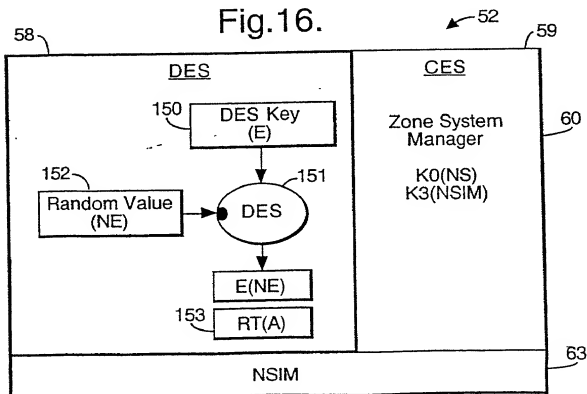


Fig.17.

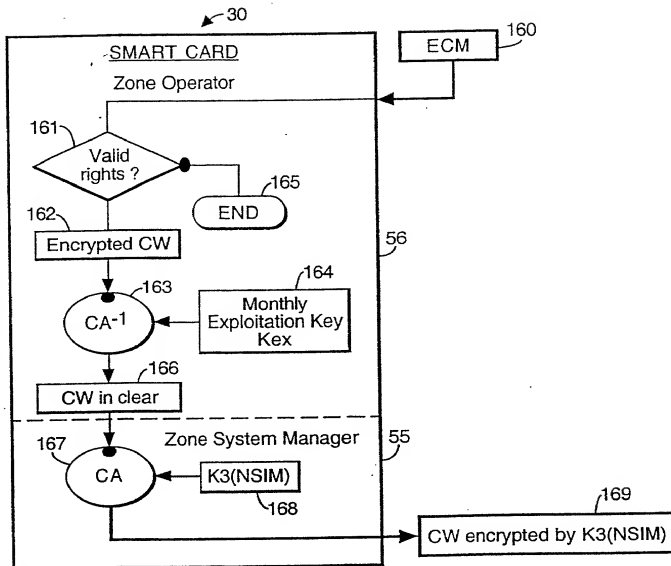


Fig.18.

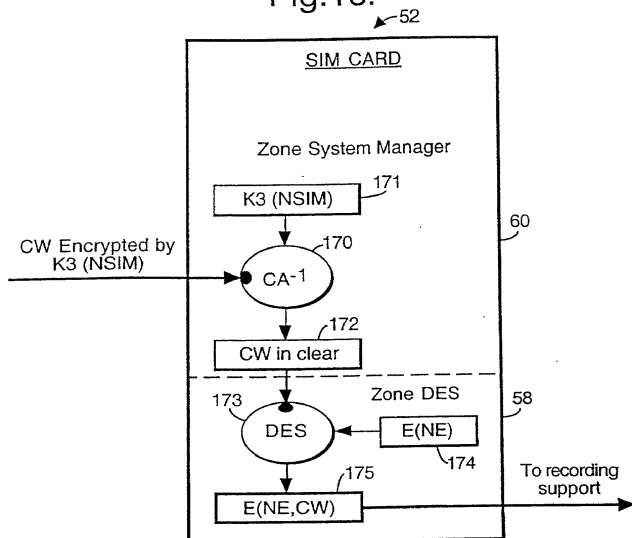
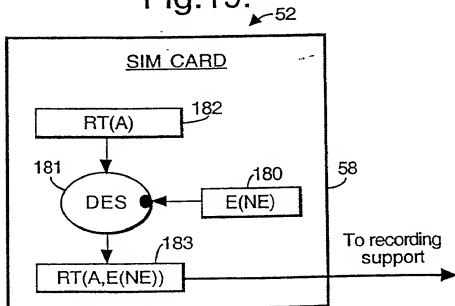
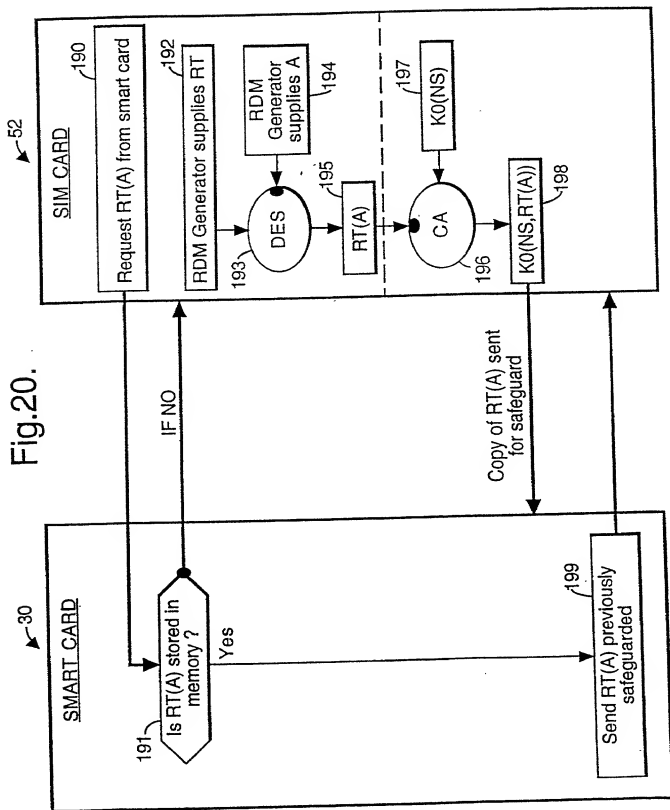


Fig.19.





Declaration and Power of Attorney for Patent Application**Déclaration et Pouvoirs pour Demande de Brevet****French Language Declaration****22511**

PATENT TRADEMARK OFFICE

En tant que l'inventeur nommé ci-après, je déclare par le présent acte que:

As a below named inventor, I hereby declare that:

Mon domicile, mon adresse postale et ma nationalité sont ceux figurant ci-dessous à côté de mon nom.

My residence, post office address and citizenship are as stated next to my name.

Je crois être le premier inventeur original et unique (si un seul nom est mentionné ci-dessous), ou l'un des premiers co-inventeurs originaux (si plusieurs noms sont mentionnés ci-dessous) de l'objet revendiqué, pour lequel une demande de brevet a été déposée concernant l'invention intitulée

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

METHOD AND APPARATUS FOR RECORDING OF
ENCRYPTED DIGITAL DATA

et dont la description est fournie ci-joint à moins que la case suivante n'ait été cochée:

the specification of which is attached hereto unless the following box is checked:

☐ a été déposée le _____
sous le numéro de demande des États-Unis ou le numéro
de demande international PCT _____
et modifiée le _____
(le cas échéant).

☐ was filed on _____
as United States Application Number or PCT
International Application Number _____
and was amended on _____
(if applicable).

Je déclare par le présent acte avoir passé en revue et compris le contenu de la description ci-dessus, revendications comprises, telles que modifiées par toute modification dont il aura été fait référence ci-dessus.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

Je reconnais devoir divulguer toute information pertinente à la brevetabilité, comme défini dans le Titre 37, § 1.56 du Code fédéral des réglementations.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

French Language Declaration

Je revendique par le présent acte avoir la priorité étrangère, en vertu du Titre 35, § 119(a)-(d) ou § 365(b) du Code des Etats-Unis, sur toute demande étrangère de brevet ou certificat d'inventeur ou, en vertu du Titre 35, § 365(a) du même Code, sur toute demande internationale PCT désignant au moins un pays autre que les Etats-Unis et figurant ci-dessous et, en cochant la case, j'ai aussi indiqué ci-dessous toute demande étrangère de brevet, tout certificat d'inventeur ou toute demande internationale PCT ayant une date de dépôt précédant celle de la demande à propos de laquelle une priorité est revendiquée.

Prior foreign application(s)
Demande(s) de brevet antérieure(s)

98400344.2 European
(Number) (Country)
(Numéro) (Pays)

98401513.1 European
(Number) (Country)
(Numéro) (Pays)

Je revendique par le présent acte tout bénéfice, en vertu du Titre 35, §119(e) du Code des Etats-Unis, de toute demande de brevet provisoire effectuée aux Etats-Unis et figurant ci-dessous.

(Application No.)
(N° de demande)

(Filing Date)
(Date de dépôt)

(Application No.)
(N° de demande)

(Filing Date)
(Date de dépôt)

Je revendique par le présent acte tout bénéfice, en vertu du Titre 35, § 120 du Code des Etats-Unis, de toute demande de brevet effectuée aux Etats-Unis, ou en vertu du Titre 35, § 365(c) du même Code, de toute demande internationale PCT désignant les Etats-Unis et figurant ci-dessous et, dans la mesure où l'objet de chacune des revendications de cette demande de brevet n'est pas divulgué dans la demande antérieure américaine ou internationale PCT, en vertu des dispositions du premier paragraphe du Titre 35, § 112 du Code des Etats-Unis, je reconnais devoir divulguer toute information pertinente à la brevetabilité, comme défini dans le Titre 37, § 1.56 du Code fédéral des réglementations, dont j'ai pu disposer entre la date de dépôt de la demande antérieure et la date de dépôt de la demande nationale ou internationale PCT de la présente demande:

PCT/IB99/00303 11 February 1999
(Application No.) (Filing Date)
(N° de demande) (Date de dépôt)

(Application No.) (Filing Date)
(N° de demande) (Date de dépôt)

Je déclare par le présent acte que toute déclaration ci-incluse est, à ma connaissance, véridique et que toute déclaration formulée à partir de renseignements ou de suppositions est tenue pour véridique; et de plus, que toutes ces déclarations ont été formulées en sachant que toute fausse déclaration volontaire ou son équivalent est passible d'une amende ou d'une incarcération, ou des deux, en vertu de la Section 1001 du Titre 18 du Code des Etats-Unis, et que de telles déclarations volontairement fausses risquent de compromettre la validité de la demande de brevet ou du brevet délivré à partir de celle-ci.

I hereby claim foreign priority under Title 35, United States Code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below, and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Priority Not Claimed
Droit de priorité revendiqué

13 February 1998 ☐
(Day/Month/Year Filed)
(Jour/Mois/Année de dépôt)

18 June 1998 ☐
(Day/Month/Year Filed)
(Jour/Mois/Année de dépôt)

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

Pending
(Status) (patented, pending, abandoned)
(Statu) (breveté, en cours d'examen, abandonné)

(Status) (patented, pending, abandoned)
(Statu) (breveté, en cours d'examen, abandonné)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

French Language Declaration

POUVOIRS: En tant que l'inventeur cité, je désigne par la présente l'(les) avocat(s) et/ou agent(s) suivant(s) pour qu'ils poursuive(nt) la procédure de cette demande de brevet et traite(nt) toute affaire s'y rapportant avec l'Office des brevets et des marques: (mentionner le nom et le numéro d'enregistrement).

Adresser toute correspondance à:

10 -

Adresser tout appel téléphonique à: (nom et numéro de téléphone)

USE ADDRESS ON
TRANSMITTAL LETTER


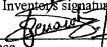
POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: (list name and registration number).

Send Correspondence to:

Jonathan P. Osha, Reg. No. 33,986; Adenike Adewuya, Reg. No. 42,254
 Alan D. Rosenthal, Reg. No. 27,833; Y. Renee Alsandor, Reg. No. 45,883
 Richard A. Fagin, Reg. No. 39,182; Jeffrey S. Bergman, Reg. No. 45,925
 K. KaRan Reed, Reg. No. 45,036; Scott W. Hejny, Reg. No. 45,882
 David E. Mixon, Reg. No. 43,809; Thomas K. Scherer, Reg. No. 45,079

Direct Telephone Calls to: (name and telephone number)

Jonathan P. Osha
 (713) 228-8600

Nom complet de l'unique ou premier inventeur	1 - 00	Full name of sole or first inventor	Michel MAILLARD
Signature de l'inventeur	Date	Inventor's signature	
Domicile		Residence	42, avenue du Marechal Leclerc, F-28130 Maintenon France
Nationalité		Citizenship	FRANCE
Adresse postale		Post Office Address	42, avenue du Marechal Leclerc, F-28130 Maintenon France
Nom complet du second co-inventeur, le cas échéant	2 - 00	Full name of second joint inventor, if any	Christian BENARDEAU
Signature du second inventeur	Date	Second Inventor's signature	 07 AOJ- 206
Domicile		Residence	13, allée des Puisatières, F-77600 Bussy Saint Georges FRANCE FR
Nationalité		Citizenship	FRANCE
Adresse postale		Post Office Address	13, allée des Puisatières, F-77600 Bussy Saint Georges FRANCE

(Fournir les mêmes renseignements et la signature de tout (Supply similar information and signature for third and co-inventeur supplémentaire.) subsequent joint inventors.)